Extremal doubly-even self-dual codes and related designs(a survey)(Theory and Applications of Combinatorial Designs with Related Field)

AUTHOR(S):

原田, 昌晃

数理解析研究所講究録 1465 巻 2006 年 1-13

Extremal doubly-even self-dual codes and related designs (a survey)

山形大・理学部 原田 昌晃 (Masaaki Harada)
Department of Mathematical Sciences
Yamagata University

1 はじめに

2 元体 $\mathbb{F}_2$ 上の n 次元ベクトル空間 $\mathbb{F}_2^n$ の k 次元部分空間を長さ n, 次元 k の binary code とよぶ (なお本原稿中での code は全て binary とする). 長さ n, 次元 k で minimum weight d の code を $[n,k,d]$ code とよぶ. code C に対して通常の内積 "$\cdot$" を考えて $C=C^{\perp}$ となるときに self-dual とよぶ. ただし $C^{\perp}=\{x\in\mathbb{F}_2^n|\ x\cdot y=0\ (\forall y\in C)\}$ である. また, 全ての codeword $x\in C$ の weight $\mathrm{wt}(x)$ が 4 の倍数であるとき C を doubly-even とよぶ. 長さ n の doubly-even self-dual code の minimum weight d は $d\leq 4[n/24]+4$ を満たし $d=4[n/24]+4$ の場合 extremal とよばれる.

本講演では extremal doubly-even self-dual code とそれらに関係した design についての survey を行なった. 本原稿では, 講演内容を簡単にまとめておく. ページ数の制限もあって全ての結果に証明を付けることは出来ないので, 講演中に紹介したものを中心に証明を与えることにする. 一般的によく使われている用語を用いているが, 紹介していない用語については [11], [12], [14], [21] などを見ていただきたい.

本原稿の構成は以下の通りである. 第 2 節では doubly-even self-dual code の weight enumerator の基本的な性質を述べて, 代数的符号理論における非常に有名な結果である Gleason の定理を紹介する. また Gleason の定理から導かれる幾つかの結果を述べる. 特に doubly-even self-dual code の minimum weight に関する上限を与え extremal を定義する. 第 3 節では, まず extremal doubly-even self-dual code の非存在の結果を紹介する. この結果も Gleason の定理から導かれる結果の一つである. その後 doubly-even self-dual code の分類に関する結果および extremal doubly-even self-dual code の存在について現時点で知られていることをそれぞれ表にまとめる. これらに関する問題も与えることにする. 第 4 節では extremal doubly-even self-dual code に関係した design について考えていく. まず Assmus–Mattson の定理を紹介し, これを用いて長さが $24m$ の場合には各 weight の codeword が 5-design になることを示す. さらにこの 5-design と同じパラメータをもつ self-orthogonal design の incidence matrix の行が生成する code が extremal doubly-even self-dual code になるか, という問題を考える. 現在のところ $m\leq 4$ までは正しいことが分かっているが, ここでは $m=1$ の場合の証明を与える.

なお self-dual code についての survey としては Rains–Sloane によるものがある [21]. 幅広く色々な話題について述べられているので, 興味のある方は目を通してみることをお

勧めしたい. また, 主に $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$ 上の self-dual code の分類と存在に関して Huffman [14] による survey がつい最近出版されたばかりである. 出版されたばかりでまだ全体に目を通していないが, こちらも参考になると思われる.

2 Gleason の定理と extremal doubly-even self-dual code

この節では doubly-even self-dual code の weight enumerator に関する非常に有名な結果である Gleason の定理を紹介する. また Gleason の定理から導くことが出来る doubly-even self-dual code の minimum weight の上限を紹介し extremal doubly-even self-dual code を定義する.

C の weight enumerator は $W_C(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$ で定義される. ただし $A_i = |\{c \in C | \operatorname{wt}(c) = i\}|$ である. 次は良く知られている.

Theorem 2.1 (MacWilliams identity). $C, C^\perp$ の weight enumerator に対して

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+y, x-y)$$

が成り立つ.

Theorem 2.2. C を長さ n の doubly-even self-dual code とすると, その weight enumerator $W_C(x,y)$ は次を満たす:

(1) $W_C(x,y) = W_C\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right)$

(2) $W_C(x,y) = W_C(x, iy)$ ここで $i = \sqrt{-1}$.

Proof. (1) C が self-dual であることから $W_C(x,y) = W_{C^\perp}(x,y)$ が成り立ち, MacWilliams identity より

$$W_{C^\perp}(x,y) = \frac{1}{2^{n/2}} W_C(x+y, x-y) = W_C\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right)$$

となることから得られる.

(2) C は doubly-even なので全ての codeword の weight は 4 の倍数である. このことから $W_C(x,y)$ は y^4 の巾だけを含むことが分かる. したがって $W_C(x,y) = W_C(x, iy)$.

以上で示せた. □

このことから $W_C(x,y)$ は次の一次変換:

$$\begin{cases} T_1 : \begin{pmatrix} x \\ y \end{pmatrix} \to \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ T_2 : \begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \end{cases}$$

によって不変であることが分かる. これらによって生成される群

$$G = \left\langle \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\rangle (\subset GL(2,\mathbb{C}))$$

を考える. この群は位数 192 の有限群であることが知られている. 次に G によって不変な多項式全体を考える:

$$\mathbb{C}[x,y]^G = \{f(x,y) \in \mathbb{C}[x,y] \mid A \circ f(x,y) = f(x,y)\ (\forall A \in G)\}$$

ここで $A \circ f(x,y)$ は $f(x,y) \in \mathbb{C}[x,y]$ の A による像を意味する. 今までの議論から次が成り立つことが分かる.

Proposition 2.3. doubly-even self-dual code C の weight enumerator $W_C(x,y)$ は $A \in G$ によって不変である. ゆえに $W_C(x,y) \in \mathbb{C}[x,y]^G$ となる.

さらに Gleason [5] は次のことを示した.

Theorem 2.4 (Gleason [5]). C を doubly-even self-dual code とする. このとき

$$W_C(x,y) \in \mathbb{C}[x,y]^G = \mathbb{C}[\phi_8, \phi_{24}]$$

ただし $\phi_8 = x^8 + 14x^4y^4 + y^8, \phi_{24} = x^4y^4(x^4 - y^4)^4$. また, ある整数 a_j を用いて

$$W_C(x,y) = \sum_{j=0}^{[n/24]} a_j {\phi_8}^{n/8-3j} {\phi_{24}}^j \tag{1}$$

と表せる.

この Gleason の定理から多くの有益な結果が導かれている. ここではその幾つかを紹介する.

Corollary 2.5. 長さ n の doubly-even self-dual code が存在するための必要十分条件は $n \equiv 0 \pmod 8$ である.

Proof. Gleason の定理よりもし長さ n の doubly-even self-dual code が存在するならば $n \equiv 0 \pmod 8$ でなければならないことが分かる. 次に長さ m, n の code C, D に対して

$$C \oplus D = \{(x,y) \in \mathbb{F}_2^{m+n} | x \in C, y \in D\}$$

と定義する. 長さ 8 の doubly-even self-dual code は同値を除いて一つだけ存在する (表 1). この code を e_8 と表すことにすると $e_8 \oplus e_8 \oplus \cdots \oplus e_8$ が長さ $8k$ の doubly-even self-dual code になる ($k = 1, 2, \ldots$). □

Theorem 2.6 (Mallows–Sloane [18]). doubly-even self-dual $[n, n/2, d]$ code に対して

$$d \leq 4[n/24] + 4$$

が成り立つ.

Proof. ここでは長さ 24 の場合の証明を考えることにする. Gleason の定理から

$$\begin{aligned} W_C(x,y) &= a_0\phi_8^3 + a_1\phi_{24} \\ &= a_0x^{24} + (42a_0 + a_1)x^{20}y^4 + (591a_0 - 4a_1)x^{16}y^8 + (2828a_0 + 6a_1)x^{12}y^{12} + \cdots . \end{aligned}$$

したがって $a_0 = 1$ でなければならない. すると

$$W_C(x,y) = x^{24} + (42 + a_1)x^{20}y^4 + (591 - 4a_1)x^{16}y^8 + (2828 + 6a_1)x^{12}y^{12} + \cdots$$

となる. ここで $d \geq 8$ とすると $x^{20}y^4$ の係数を考えることで $a_1 = -42$ が得られる. したがって

$$W_C(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}$$

であり $d \leq 8$ を得る.

一般の場合も本質的には同じで minimum weight から (1) において $a_0, a_1, \ldots, a_{[n/24]}$ を決めることで上限を得る. □

Definition 2.7. doubly-even self-dual $[n, n/2, 4[n/24] + 4]$ code を *extremal* とよぶ.

3 Extremal doubly-even self-dual code の分類および存在について

この節ではまず始めに長さ n が非常に大きな extremal doubly-even self-dual code の非存在について紹介する. 次に doubly-even self-dual code の分類についての結果を与えて, 最後に extremal doubly-even self-dual code の存在について現在のところ分かっていることをまとめておく.

3.1 非存在について

Zhang [26] は Gleason の定理を用いて extremal doubly-even self-dual code の weight enumerator を求めて $A_{4[n/24]+8}$ (weight $4[n/24] + 8$ の codeword の個数) が負になることを確かめることで次を得た.

Theorem 3.1 (Zhang [26]). $n = 24m$ $(m \geq 154)$, $n = 24m + 8$ $(m \geq 159)$, $n = 24m + 16$ $(m \geq 164)$ のとき, 長さ n の extremal doubly-even self-dual code は存在しない.

Problem 1. 別の weight を考えることで上に与えられた長さより小さなところでの非存在を示すことが出来るか.

現在のところ, 上の結果以外に extremal doubly-even self-dual code の非存在については知られていない.

3.2 分類について

長さ 32 以下の doubly-even self-dual code についての分類が完成している. 結果だけであるが表 1 に与えることにする. ただし, 表中の第 2 列「#(Extremal)」は非同値な extremal doubly-even self-dual code の個数を, 第 4 列「#(全て)」は extremal を含めて全ての非同値な doubly-even self-dual code の個数を表す. また第 3 列には良く用いられる code の記号を与えておく. e_8 は extended Hamming $[8,4,4]$ code, g_{24} は extended Golay $[24,12,8]$ code とよばれる code である.

表 1: doubly-even self-dual code の分類結果

長さ	#(Extremal)	code	#(全て)	文献
8	1	e_8	1	[19]
16	2	d_{16}^+, e_8^2	2	[19]
24	1	g_{24}	9	[20]
32	5	C81,..., C85	85	[3]

self-dual code の分類に関しては mass formula とよばれる等式が成り立つことが知られている. 非常に面白い結果であるが講演中にも触れなかったので, これについては言及しないこととする (例えば [3] を参照).

3.3 Design を用いた構成方法

doubly-even self-dual code の構成方法については色々なものが知られている. ここでは design が本研究集会の主たる対象であったので design を用いた doubly-even self-dual code の構成方法を与える.

Proposition 3.2 (Tonchev [24] 参照). A を symmetric 2-(v,k,λ) design の incidence matrix とする.

(1) $k \equiv 3 \pmod 4$, $\lambda \equiv 0 \pmod 2$ であるとき $G = (\ I\ \ A\ )$ は長さ $2v$ の doubly-even self-dual code を生成する.

(2) $k \equiv 2 \pmod 4$, $\lambda \equiv 1 \pmod 2$ であるとき

$$G = \begin{pmatrix} & 0 & 1 & \cdots & 1 \\ & 1 & & & \\ I & \vdots & & A & \\ & 1 & & & \end{pmatrix}$$

は長さ $2v+2$ の doubly-even self-dual code を生成する.

Proof. どちらの場合も, G の各行の weight が 4 の倍数であることと G の異なる 2 行が直交することから doubly-even self-dual code になることが直ちに分かる. □

Remark 3.3. 上から直接得られる symmetric 2-(v,k,λ) design の非存在についての結果を講演中に紹介したが, その結果は完全に Bruck–Ryser–Chowla の定理に含まれることを集会中に平峰豊氏 (熊本大) と宗政昭弘氏 (東北大) からご教授いただいた. お二方に感謝します.

例えば Hadamard 2-$(11,6,3)$ design を考えると (2) によって extremal doubly-even self-dual $[24,12,8]$ code g_{24} が得られる. また symmetric 2-$(31,10,3)$ design から 4 つの非同値な長さ 64 の extremal doubly-even self-dual code が得られることが知られている [15].

Proposition 3.4 (Tonchev [25]). H を位数 $8t+4$ の Hadamard 行列とする. H の各行の 1 の個数が $4k+3$ であるとき

$$\begin{pmatrix} I & \frac{H+J}{2} \end{pmatrix}$$

は長さ $16t+8$ の doubly-even self-dual code を生成する. ただし J は全ての成分が 1 である行列を表す.

位数 28 以下の Hadamard 行列の分類は完成している. 上の方法によって位数 20, 28 の Hadamard 行列よりそれぞれ 118, 5 個の非同値な extremal doubly-even self-dual code が得られることが分かっている [2], [16].

3.4 存在について

extremal doubly-even self-dual code の存在について表 2 にまとめておく. 表において # は現在のところ知られている非同値な extremal doubly-even self-dual code の個数を表す. なお, 文献に関しては最新のものを一つだけ挙げている. 全ての extremal doubly-even self-dual code については挙げられている文献の参考文献を参照していただきたい. 特に分類が終わっている長さ 32 以下を除いて次の場合のみ分類が完成していることを注意しておく.

Theorem 3.5 (Houghten–Lam–Thiel–Parker [13]). 全ての長さ 48 の extremal doubly-even self-dual code は extended quadratic residue code と同値になる.

表 2: extremal doubly-even self-dual code の存在

長さ	#	文献	長さ	#	文献
40	≥ 12579	[17]	96	?	-
48	1	[13]	104	≥ 1	[21] 参照
56	≥ 1151	[9]	112	?	-
64	≥ 3270	[10]	120	?	-
72	?	-	128	?	-
80	≥ 15	[7]	136	≥ 1	[21] 参照
88	≥ 470	[6]	144	?	-

直ちに次のようなことが考えられる.

Problem 2. 存在の決まっていない長さにおいて extremal doubly-even self-dual code が存在するかどうかを決定せよ.

Problem 3. 長さ 40 の extremal doubly-even self-dual code の分類は可能か.

Problem 4. 各長さに関して, 表 2 を改良せよ.

長さが 100 を超えるところでは存在が分かっていない場合が多い. これは今まで研究対象とされて来なかったことと minimum weight を決定するのが困難であるという計算量の問題であると思われる. extremal の定義とその前後の状況から考えて長さ 112 については extremal が存在すると個人的には考えているが, 現在のところ構成は出来ていない (幾つかの方法で何度かチャレンジしているのだが). 特に, この長さは問題として強調しておく.

Problem 5. 長さ 112 の extremal doubly-even self-dual code を構成せよ.

また, 長さ 96 以下で存在が決まっていないのは長さが 24 の倍数の場合のみで, 特に長さ 72 の場合に存在性を決めるのは古くから知られている有名な問題である [22]. 次節で, 長さ $24m$ の extremal doubly-even self-dual code に関係した design について考えていく.

3.5 長さ 72 の場合

上で述べた通り長さ 72 の extremal doubly-even self-dual code の存在については未解決であるが, 既に分かっている幾つかの性質についてここで述べておく.

- weight enumerator:

Gleason の定理から weight enumerator $W_C(x,y)$ は決定される. ここでは $W_C(1,y)$ を与えておく:

$$W_C(1,y) = 1 + 249849y^{16} + 18106704y^{20} + 462962955y^{24} + 4397342400y^{28} + 16602715899y^{32} + 25756721120y^{36} + \cdots + y^{72}.$$

- 他の長さの self-dual code との関係:

  Proposition 3.6 (Dougherty–Harada [4]). (1) 長さ 72 の extremal doubly-even self-dual code の存在と self-dual $[70, 35, 14]$ code の存在は同値である.

  (2) もし長さ 72 の extremal doubly-even self-dual code が存在すれば $W_C(1,y) = 1 + 442y^{12} + 14960y^{14} + 174471y^{16} + \cdots$ である self-dual $[68, 34, 12]$ code が存在する.

  Problem 6. (2) の逆は成り立つか.

- 自己同型について:

  長さ 72 の extremal doubly-even self-dual code の自己同型についても古くから研究が行なわれているので, 結果だけは紹介することにする. 自己同型となり得る奇素数の位数の可能性は $3, 5, 7$ だけであり, 位数 $5, 7$ の場合は 2 つの固定点を持ち, 位数 3 の場合は固定点を持たないことが分かっている (詳しくは [14] を参照).

4 長さ $24m$ の extremal doubly-even self-dual code と 5-design

前節では $m = 1, 2$ の場合のみ長さ $24m$ の extremal doubly-even self-dual code が同値を除いて一つだけ存在し, $m = 3, 4, 5, \ldots, 153$ の場合は存在性が決められていないことを述べた. この節では, これらに関係した design について考えていく.

4.1 Assmus–Mattson の定理

Theorem 4.1 (Assmus–Mattson [1]). C を $[n, k, d]$ code とし $0 < t < d$ とする. $B_i = \#\{x \in C^\perp \mid \mathrm{wt}(x) = i\}$, $s = \#\{i \mid B_i \neq 0 \text{ and } 0 < i \leq n - t\}$ としたとき, もし $s \leq d - t$ であれば

(1) C の weight d の codeword (の support) は t-design になる.

(2) $C^\perp$ の任意の weight i $(i \leq n - t)$ の codeword (の support) は t-design になる.

Assmus–Mattson の定理より直ちに次が得られる.

Corollary 4.2. C を長さ $24m$ の extremal doubly-even self-dual code とすると, 各 weight の codeword は 5-design になる.

Proof. $t = 5$ と仮定する. C の $24m - 5$ 以下の codeword が存在する可能性のある weight は

$$4m + 4, 4m + 8, 4m + 12, \ldots, 24m - (4m + 4).$$

したがって $s \leq 4m - 1$ であるので Assmus–Mattson の定理の仮定を満たす. □

$m = 1, 2, 3, 4$ の場合の minimum weight の codeword がなす 5-design のパラメータを表 3 に与えておく. A_{4m+4} は weight $4m + 4$ の codeword の個数, つまり design の block の個数を表す.

表 3: 5-design のパラメータ

m	A_{4m+4}	5-design のパラメータ
1	759	$S(5, 8, 24)$
2	17296	5-$(48, 12, 8)$ design
3	249849	5-$(72, 16, 78)$ design
4	3217056	5-$(96, 20, 816)$ design

Assums–Mattson の定理によってもし extremal doubly-even self-dual code が存在すれば 5-design が得られる. では, その逆はどうなっているのであろうか. 以下このことについて考えていく.

4.2 $m = 1$ の場合

Steiner system $S(5, 8, 24)$ は s-$(24, 8, \lambda_s)$ design になる $(s \leq 5)$, ここで

$$b = \lambda_0 = 759, \lambda_1 = 253, \lambda_2 = 77, \lambda_3 = 21, \lambda_4 = 5$$

となる.

Lemma 4.3. Steiner system $S(5, 8, 24)$ の任意の異なる 2 つの block の共通部分の濃度 (block intersection number と呼ぶ) は丁度 $0, 2, 4$ である.

Proof. B を $S(5, 8, 24)$ の任意の block とし, m_i を B との交わりが i point である B 以外の block の総数とする. ここで同じ block は存在しないので $0 \leq i \leq 7$ である. 5-design であることから交わりの部分の point の個数を二通りに数えることによって次の連立方程式が得られる:

$$\sum_{i=0}^{7} \binom{i}{j} m_i = (\lambda_j - 1)\binom{8}{j} \quad (j = 0, 1, \ldots, 5).$$

この連立方程式の解は

$$m_0 = 30 + m_6 + 6m_7, m_1 = -6m_6 - 35m_7, m_2 = 448 + 15m_6 + 84m_7,$$
$$m_3 = -20m_6 - 105m_7, m_4 = 280 + 15m_6 + 70m_7, m_5 = -6m_6 - 21m_7$$

と表せる. ここで m_i は 0 以上の整数であるので, 最後の式より $m_5 = m_6 = m_7 = 0$ が得られる. したがって

$$m_0 = 30, m_1 = 0, m_2 = 448, m_3 = 0, m_4 = 280$$

となる. □

次はよく知られている結果であるが, ここでは (著者が知っている限りではあるが) 連立方程式だけを考えれば済む新しい証明を紹介する.

Theorem 4.4. Steiner system $S(5,8,24)$ の incidence matrix の行が生成する code は extended Golay $[24,12,8]$ code に同値になる.

Proof. Steiner system $S(5,8,24)$ の incidence matrix を A とおき A の行が生成する code を C で表すことにする. Lemma 4.3 と block size が 8 であることより C は doubly-even self-orthogonal になることがただちに分かる.

次に $w \in C^\perp$ を weight $m > 0$ の codeword とする. w との交わりが i 列である A の行の総数を n_i とする. このとき, 5-design であることから次の連立方程式を得る:

$$\sum_{i=0}^{[m/2]} \binom{2i}{j} n_{2i} = \lambda_j \binom{m}{j} \quad (j = 0, 1, \ldots, 5). \tag{2}$$

ここで $n_{2i} = 0$ $(i \geq 5)$ と $n_{2k+1} = 0$ であることに注意しておく. この連立方程式 (2) が解をもつ条件は

$$m(m^4 - 60m^3 + 1280m^2 - 11520m + 36864)$$
$$= m(m-8)(m-12)(m-16)(m-24) = 0$$

であることが分かる.

方程式 (2) の解は $m = 0, 8, 12, 16, 24$ であることより $C^\perp$ において codeword が存在する可能性のある weight は $0, 8, 12, 16, 24$ だけであることが分かる (ここで Lemma 4.3 と C が self-orthogonal であることより実際に $C^\perp$ は weight $8, 12, 16, 24$ の codeword を含むことが分かる). したがって $C^\perp$ は doubly-even code になる. doubly-even code は self-orthogonal code なので $C^\perp \subset (C^\perp)^\perp = C$ となる. つまり C は self-dual になる. $C^\perp$ での weight の可能性より minimum weight は 8 であることも直ちに分かる.

以上より C は extremal doubly-even self-dual $[24,12,8]$ code になり, 分類結果より C は extended Golay code g_{24} に同値になることが分かる. □

extremal doubly-even self-dual $[24,12,8]$ code の一意性より直ちに次を得る:

Corollary 4.5. Steiner system $S(5,8,24)$ は同型を除いてただ一つである.

4.3 一般の場合 ($m \geq 2$)

C を長さ $24m$ の extremal doubly-even self-dual code とすると, 先に述べた通り Assmus–Mattson の定理によって minimum weight の codeword は 5-design D をなす. さらに C が self-dual であることから, この design D は self-orthogonal になる. 一般に t-(v, k, λ) design が self-orthogonal であるとは, 全ての block intersection number と block size k の偶奇が一致する場合をいう [23]. 次のようなことを考えてみたい.

Problem 7. C を長さ $24m$ の extremal doubly-even self-dual code とし, D を C の minimum weight の codeword がなす self-orthogonal 5-design とする. E を D と同じパラメータをもつ任意の self-orthogonal 5-design としたとき E の incidence matrix の行が生成する code は extremal doubly-even self-dual code になるか.

$m = 1$ のときは Theorem 4.4 より正しいことが分かる. それぞれ $m = 2, 3, 4$ の場合にも正しいことが次の最近の論文の中で示されている [12], [11], [8] (この辺りについての日本語の記事は [27], [28]).

Theorem 4.6 ([8], [11], [12]). (1) 任意の self-orthogonal 5-$(48, 12, 8)$ design の incidence matrix の行は extremal doubly-even self-dual $[48, 24, 12]$ code を生成する. また self-orthogonal 5-$(48, 12, 8)$ design は同型を除いて一意的に存在する.

(2) もし self-orthogonal 5-$(72, 16, 78)$ design が存在すれば incidence matrix の行が生成する code は extremal doubly-even self-dual $[72, 36, 16]$ code になる.

(3) もし self-orthogonal 5-$(96, 20, 816)$ design が存在すれば incidence matrix の行が生成する code は extremal doubly-even self-dual $[96, 48, 20]$ code になる.

$m \leq 4$ の場合には正しいことが分かったが $m \geq 5$ において正しいのだろうか (著者は正しくあって欲しいという願望をもっているが). 証明の中で主に考えたことは連立方程式 (2) を用いることであった. これは考えている design E が 5-design である性質を十分反映させていると思う. しかしながらこの問題を一般的に考えるには, まだまだ何かが足りないように思えるので, 今後その辺りを考えていきたい. また, 上記の問題を考えることは extremal doubly-even self-dual code の存在性を決定するのに有効なアプローチであって欲しいと願っているが, 今のところ, 全く分からない. 何とか長さ 72 の場合の存在性の決定への足掛かりになればと思っている.

最後に, 本研究集会の研究代表者の篠原聡氏の計らいで本講演を 2004 年 Hall メダル受賞記念講演とさせて貰いました. このような機会を下さった篠原聡氏に心から感謝します. また, 集会中にお祝いの言葉を掛けて下さった皆様にもこの場を借りてお礼を述べさせていただきます. 原稿を読んでコメントをくれた新谷誠氏と宮林寛樹氏にも感謝します.

参考文献

[1] E.F. Assmus, Jr. and H.F. Mattson, Jr., New 5-designs, *J. Combin. Theory* **6** (1969), 122–151.

[2] F.C. Bussemaker and V.D. Tonchev, Extremal doubly-even codes of length 40 derived from Hadamard matrices of order 20, *Discrete Math.* **82** (1990), 317–321.

[3] J.H. Conway, V. Pless and N.J.A. Sloane, The binary self-dual codes of length up to 32: a revised enumeration, *J. Combin. Theory Ser. A* **60** (1992), 183–195.

[4] S.T. Dougherty and M. Harada, New extremal self-dual codes of length 68, *IEEE Trans. Inform. Theory* **45** (1999), 2133–2136.

[5] A.M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, Actes Congrés Intern. Math. (Nice, 1970), pp. 211–215. Gauthier-Villars, Paris, 1971.

[6] T.A. Gulliver and M. Harada, Classification of extremal double circulant self-dual codes of lengths 74 to 88, (submitted).

[7] T.A. Gulliver, M. Harada and J.-L. Kim, Construction of new extremal self-dual codes, *Discrete Math.* **263** (2003), 81–91.

[8] M. Harada, Remark on a 5-design related to a putative extremal doubly-even self-dual $[96, 48, 20]$ code, *Designs, Codes and Cryptogr.* (2005), to appear.

[9] M. Harada, Self-orthogonal 3-$(56, 12, 65)$ designs and extremal doubly-even self-dual codes of length 56, *Designs, Codes and Cryptogr.* (2005), to appear.

[10] M. Harada and H. Kimura, New extremal doubly-even $[64, 32, 12]$ codes, *Designs, Codes and Cryptogr.* **6** (1995), 91–96.

[11] M. Harada, M. Kitazume and A. Munemasa, On a 5-design related to an extremal doubly even self-dual code of length 72, *J. Combin. Theory Ser. A* **107** (2004), 143–146.

[12] M. Harada, A. Munemasa and V.D. Tonchev, A characterization of designs related to an extremal doubly-even self-dual code of length 48, *Ann. Combin.* **9** (2005), 189–198.

[13] S.K. Houghten, C.W.H. Lam, L.H. Thiel and J.A. Parker, The extended quadratic residue code is the only $(48, 24, 12)$ self-dual doubly-even code, *IEEE Trans. Inform. Theory* **49** (2003), 53–59.

[14] W.C. Huffman, On the classification and enumeration of self-dual codes, *Finite Fields Appl.* **11** (2005), 451–490.

[15] S.N. Kapralov and V.D. Tonchev, Extremal doubly-even codes of length 64 derived from symmetric designs, *Discrete Math.* **83** (1990), 285–289.

[16] H. Kimura, Extremal doubly even $(56, 28, 12)$ codes and Hadamard matrices of order 28, *Australas. J. Combin.* **10** (1994), 153–161.

[17] O.D. King, The mass of extremal doubly-even self-dual codes of length 40, *IEEE Trans. Inform. Theory* **47** (2001), 2558–2560.

[18] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Inform. Control* **22** (1973), 188–200.

[19] V. Pless, A classification of self-orthogonal codes over $GF(2)$, *Discrete Math.* **3** (1972), 209–246.

[20] V. Pless and N.J.A. Sloane, On the classification and enumeration of self-dual codes, *J. Combin. Theory Ser. A* **18** (1975), 313–335.

[21] E. Rains and N.J.A. Sloane, "Self-dual codes," Handbook of Coding Theory, V.S. Pless and W.C. Huffman (Editors), Elsevier, Amsterdam 1998, pp. 177–294.

[22] N.J.A. Sloane, Is there a $(72, 36)$ $d = 16$ self-dual code? *IEEE Trans. Inform. Theory* **19** (1973), 251.

[23] V.D. Tonchev, A characterization of designs related to the Witt system $S(5, 8, 24)$, *Math. Z.* **191** (1986), 225–230.

[24] V.D. Tonchev, Symmetric designs without ovals and extremal self-dual codes, *Combinatorics '86* (Trento, 1986), 451–457, *Ann. Discrete Math.* **37**, North-Holland, Amsterdam, 1988.

[25] V.D. Tonchev, Self-orthogonal designs and extremal doubly even codes, *J. Combin. Theory Ser. A* **52** (1989), 197–205.

[26] S. Zhang, On the nonexistence of extremal self-dual codes, *Discrete Appl. Math.* **91** (1999), 277–286.

[27] 原田昌晃, On a 5-design related to an extremal doubly-even self-dual code, 第 22 回代数的組合せ論シンポジウム報告集 (2005), 印刷中.

[28] 原田昌晃, 北詰正顕, 宗政昭弘, 長さ 72 の extremal doubly-even self-dual code に関係した 5-design について, 第 21 回代数的組合せ論シンポジウム報告集 (2004), 88–94.